AO 106A (EDVA Version) (03/20) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
165 Merrimac Trail, Apt. 6, Williamsburg, VA, 23185

Case No. 4:20sw43

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 USC § 2252A(a)(2)	Receipt and Distribution of child pornography
Title 18 USC § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See Affidavit

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Reviewed by AUSA/SAUSA

Peter Osyf
Printed name and title

Stacey A. Sullivan, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

_____ *(specify reliable electronic means).*

Date: April 16, 2020

Judge's signature

City and state: Norfolk, VA

Lawrence R. Leonard
United States Magistrate Judge
Printed name and title

FILED UNDER SEAL PURSUANT TO THE E-GOVERNMENT ACT OF 2002

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

Introduction and Agent Background

I, Stacey Sullivan, being duly sworn, hereby depose and state:

1. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation (FBI). I have been employed by the FBI has a Special Agent since October 2008. As such, I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, § 2510 (7). That is, I am an officer of the United States, who is empowered by law to conduct investigations regarding violations of United States law, to execute warrants issued under the authority of the United States, and to make arrests of the offenses enumerated in Title 18, United States Code, § 2251 *et seq.* In the course of my duties, I am responsible for investigating crimes which include, but are not limited to, child exploitation and child pornography. I have previously been involved in criminal investigations concerning violations of federal laws. Since joining the FBI, your affiant has received specialized training in human trafficking investigations, identifying and seizing electronic evidence, computer forensics, recovery, and social site investigations.

2. The information set forth in this affidavit is known to me as a result of an investigation personally conducted by me and other law enforcement agents. Thus, the statements in this affidavit are based in part on information provided by Special Agents ("SAs") and other employees of the FBI, as well as other investigators employed by federal or state governments. I have participated in investigations involving persons who collect and distribute child pornography, and the importation and distribution of materials relating to the sexual exploitation of children. I have received training in the areas of child exploitation, and I have reviewed images and videos of

child pornography in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers.

3. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws.

Location

4. This affidavit is made in support of an application for a warrant to search the entire premises located at **165 Merrimac Trail, Apartment 6, Williamsburg, VA, 23185** (more precisely described in Attachment A).

5. This affidavit is based upon information that I have gained from my investigation, my training and experience, as well as information gained from conversations with other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities (more precisely described in Attachment B) of violations of Title 18, United States Code, §§ 2252A(a)(2) and 2252A(a)(4)(B) are located at the above address.

Pertinent Federal Criminal Statutes

6. This investigation concerns alleged violation of Title 18, United States Code §§ 2252A(a)(2) and 2252A(a)(4)(B) relating to the distribution and receipt of child pornography.

7. Title 18 U.S.C. §§ 2252A(a)(2) prohibits a person from knowingly transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate

or foreign commerce by any means including by computer or mails, any visual depiction of minors engaging in sexually explicit conduct.

8. Title 18 U.S.C. §§ 2252A(a)(5)(B) prohibits a person from knowingly possessing, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

Definitions

9. The term "computer", as used herein, is defined pursuant to Title 18, United States Code, § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

10. The term "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

11. The terms "records," "documents," and "materials" include all information recorded in any form, including the originals and all non-identical copies thereof, whether different

from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

> Graphic records or representations, photographs, pictures, images, and aural records or representations.

12. The terms "minor" and "sexually explicit conduct" are defined in Title 18, United States Code, § 2256(1) and (2). A "minor" is defined as "any person under the age of eighteen years." The term "sexually explicit conduct" means actual or simulated:

i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

ii. Bestiality;

iii. Masturbation;

iv. Sadistic or masochistic abuse; or

v. Lascivious exhibition of the genitals or pubic area of any person.

13. The term "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

14. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

15. The term "Universal Resource Locator (URL)" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

16. Internet Protocol Address (IP Address): Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. There are two types of IP addresses, static and dynamic. A static address is permanent and never changes, such as ones used in cable modems. The dynamic address changes almost every time the computer connects to the Internet.

17. "Domain name system" (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function. A Dynamic DNS (DDNS) is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DNS configuration of its configured hostnames, addresses or other information.

18. The term "Internet Service Provider" (ISPs) refers to individuals who have an Internet account and an Internet-based electronic mail (e-mail) address must have a subscription, membership, or affiliation with an organization or commercial service which provides access to

the Internet. A provider of Internet access and services is referred to as an Internet Service Provider or "ISP".

19. The term "Secure Hash Algorithm" (SHA-1) is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard. SHA-1 is the original 160-bit hash function. It was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. The SHA-1 value is one form of an electronic fingerprint for a digital image.

20. "Web hosts" provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a Website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

21. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. Title 18 U.S.C. § 2510(15).

22. "Remote Computing Service" is a service that provides to the public computer storage or processing services by means of an "electronic communications system." Title 18 U.S.C. § 2711.

23. "Electronic Communications System" means any wire, radio, electromagnetic, photo optical, or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Title 18 U.S.C. § 2510(14).

24. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. Title 18 U.S.C. § 2510(8).

25. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. Title 18 U.S.C. § 2510(17).

26. The term "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

27. The term "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet.

28. The tern "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

29. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

30. Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

31. The term "Secure Shell" ("SSH"), as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

32. "Network Attached Storage" ("NAS") is a file-level computer data storage server connected to a computer network providing data access to a group of clients. A NAS not only operates as a file server, but is specialized for this task either by its hardware, software, or configuration of those elements. A NAS is often a specialized computer built for storing and serving files, rather than simply a general purpose computer being used for the role.

33. Structured Query Language ("SQL") is a special-purpose programming language designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS). SQL is used to communicate with a database. According to the American National Standards Institute ("ANSI"),

SQL is the standard language for relational database management systems. SQL statements are used to perform tasks such as update data on a database, or retrieve data from a database. Some common relational database management systems that use SQL are: Oracle, Sybase, Microsoft SQL Server, Access, Ingres, among others. SQL-DB is a log of the SQL activity.

Specifics of Search and Seizure of Computer System and Related Media

34. Your affiant, based on conversations with Computer Investigative Specialists, who have been trained in the seizure, examination and retrieval of data from personal computer systems and related media, knows that searching and seizing information from computer systems often requires agents to seize all electronic storage devices to be searched later in a laboratory or other controlled environment.

35. Computer storage devices (like hard drives, diskettes, tapes, laser disks, and thumb or flash drives) can store enormous quantities of information. For instance, a single 200-gigabyte hard-drive may contain the electronic equivalent of hundreds of thousands of pages of double-spaced text. However, unlike the search of documentary files, computers store data in files that are often not easily reviewed. Additionally, a suspect may try to conceal criminal evidence by storing files in random order and/or with deceptive file names. This may require the examiner to examine all the stored data to determine which particular files are evidence or instrumentalities of the crime. This sorting process can take weeks or months, depending on the volume of data stored.

36. Searching computer systems for criminal evidence is a highly technical process, requiring specialized skills and a properly controlled environment. The vast array of computer hardware and software available requires even computer examiners to specialize in some systems and applications, so it is difficult to know before a search which computer investigative specialist is qualified to analyze the system and its data. In any event, the investigative specialist will use

certified forensic tools and data search protocols that are designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (from external sources and/or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

37. An important step that is ordinarily part of an examiner's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.

Characteristics of Collectors of Child Pornography

38. Through my discussions with law enforcement officers who specialize in the investigation of child pornography, and of subjects who utilize web based bulletin boards to gain access to child pornography, I have learned that individuals who use such technology are often child pornography collectors who download images and videos of child pornography. Moreover, I have learned that many subjects have saved numerous images to their hard drive, thumb drive, disks or CDs, and have kept that material for long periods of time. Based upon my knowledge, experience and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, in other visual media or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Collectors of child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica[1], and videotapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

---

[1] According to former FBI Special Agent Kenneth V. Lanning, the author of a chapter in the book, Child Pornography and Sex Rings, (Lexington Books 1984), a book which deals with the subject of child pornography and pedophiles who collect and produce child pornography, "child erotica" are materials or items which are sexually arousing to pedophiles but which are not in and of themselves obscene or which do not necessarily depict minors in sexually explicit poses or positions. He defines it in the above book as: any material, relating to children, that is sexually arousing to a given individual...[s]ome of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids. Id. at 83.

Use of Computers with Child Pornography

39. Based upon my training and information officially supplied to me by other law enforcement officers, your affiant knows the following:

40. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. They have also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

41. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution and storage.

a. Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow as methods that have been used in the past.

b. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer has also changed that. A device known as a modem allows any computer to connect to another computer using telephone lines or other cable lines. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host computers are sometimes operated by commercial concerns, such as Microsoft and America Online, which allow subscribers to access their network services via connection through an Internet broadband provider or by dialing a local number and connecting via a telephone modem.

c. These service providers allow electronic mail ("e-mail") service between subscribers and between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web; hence, they are commonly described as Internet Service Providers (ISPs). Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time using a mode of communication called instant messaging, or "IM." When logged into an IM service, users can search for other users based on the information that the other users have supplied, and they can send those users messages or initiate a chat session. Chat sessions can occur in multiple person groups, or in private one-on-one sessions. Most IM services also allow files to be transferred between users, including image files.

d. These communications structures are ideal for the child pornography collector. The open and anonymous communication allows users to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send text messages and graphic images to other trusted child pornography collectors. Moreover, the child pornography collectors can use standard Internet connections, such as those provided by business, universities, and government agencies, to communicate with each other and to distribute pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornography collectors.

e. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred (via electronic mail, through file transfer protocols (FTPs), or via news group postings) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, and easy access to the Internet, the computer is a preferred method of distribution of child pornographic materials.

42. The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of five hundred (500) gigabytes are not uncommon. These drives can store hundreds of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

43. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for extended periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically

maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

44. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

Background of the Investigation and Probable Cause

45. On September 10, 2019, the National Center for Missing and Exploited Children (NCMEC) processed CyberTip 53019425 and passed it to FBI Headquarters. CyberTIp #53019425 contained 72 files uploaded and described as apparent child pornography to Dropbox, Inc. The CyberTip listed the suspect information as email address: cassidytimmy@yahoo.com, screen name: Tom Nassidy, and IP address: 2600:8805:3800:2580:5d88:8d94:7893:7038 on December 21, 2018 00:02:22 UTC. The incident time reported was listed as July 30, 2019 at 23:11:39 UTC. The incident date/time is set to 24 hours before the report was sent from Dropbox to NCMEC.

46. On September 11, 2019, FBI Headquarters issued an administrative subpoena was issued to Dropbox, Inc for email address: cassidytimmy@yahoo.com; screen/user name: Tom Nassidy; ESP User ID: 493425319. Dropbox, Inc.

47. On the same date, an administrative subpoena was issued to Cox Communications for IP address 2600:8805:3800:2580:5d88:8d94:7893:7038 on December 21, 2018 00:02:22 UTC. On September 30, 2019, Cox Communications provided customer information related to IP address 2600:8805:3800:2580:5d88:8d94:7893:7038 on December 21, 2018 00:02:22 UTC as Timothy Cassidy, 163 Merrimac Trail, Apartment 3, Williamsburg, VA, 23185.

48. The CyberTip was then sent to the Southern Virginia Internet Crimes Against Children Task Force who in turn forwarded it, based on the location of the IP address, to Investigator Todd Iverson with the Gloucester County Sheriff's office in December 2019. Once Inv. Iverson determined the IP address geo-located to a residence in Williamsburg, VA, he informed Williamsburg Police Department Investigator Alexander Willetts and the two investigators worked the CyberTip together.

49. Through further investigation, the investigators identified Timothy Cassidy as an assistant manager of a 7-11 in Williamsburg, Virginia. Cassidy resided in Williamsburg, VA at the time of the offense.

50. On or about January 2, 2020, based on a previous complaint Cassidy had filed regarding counterfeit money, Inv. Iverson and Willetts interviewed him at 7-11. During the interview, Cassidy disclosed he had moved to Newport News, VA.

50. On January 6, 2020, Inv. Iverson and Willetts met with your affiant and provided her with CyberTip 53019425 as Cassidy had moved out of their jurisdiction. At this time, Inv. Willets informed your affiant he had sent a search warrant to Dropbox, Inc. on January 3, 2020, and was

waiting for a return. Your affiant reviewed the 72 CyberTip Dropbox image and video files and determined 59 of them to be child pornography. Examples of those images contained in CyberTip 53019425 are described as follows:

a. A video file titled, "4bf88d93-813e-4edc-9d31-4e81612fee82":

The video is 6 seconds in length and depicts a nude female infant/toddler. An adult face is seen performing oral sex on her.

b. An image file titled, "0713458f-0C40-4ab4-a965-29548c0eeb22.jpg"

This image depicts an infant female with her legs apart, the camera is focused on her genitals. A sign underneath her reads SARAhWA.

51. On or about January 13, 2020, Inv. Willetts received the Dropbox search warrant return and provided it to your affiant. Your affiant reviewed the images and there were more than 200 image and video files containing child pornography. Dropbox provided the customer information as: name Tom Nassidy, email address cassidytimmy@yahoo.com, joined November 22, 2015, and the current account status was listed as disabled. A sample of those image and video files are described as follows:

a. A video file titled: VID20150626-WA0035.mp4

This video is 45 seconds in length and depicts a pre-pubescent female juvenile performing oral sex on an adult male. The male guides her head with his hand and ejaculates in her mouth.

b. A video file titled: VID-20150711-WA0031.mp4

This video is 45 seconds in length and depicts a pre-pubescent female toddler lying on her back nude from the waist down. An adult male penis is seen penetrating her anally and rubbing against her genitals.

c. A video file titled: Video Aug 11, 9 54 24 AM.mp4

This video is one minute and 35 seconds in length and depicts a pre-pubescent male juvenile lying on his back, nude from the waist down. An adult male is seen performing oral sex on the boy. The video ends with a close up of the boy's genitals/anus.

d. A video file titled: Video Aug 14, 6 27 52 PM.mp4

This video is 37 seconds in length and depicts a juvenile female, nude from the waist down. An adult male is rubbing his penis over her genitals and masturbating himself.

52. On March 24, 2020, James City County Task Force Officer Richard Pennycuff conducted a physical surveillance at the apartment building located at 165 Merrimac Trail, Williamsburg, VA. TFO Pennycuff observed a Volkswagen Golf GTI bearing Virginia Tags: UKR-1495 parked in front of the complex. A check with the Virginia Department of Motor Vehicles revealed the 2015 white Volkswagen was registered to Timothy Michael Cassidy and Heather Marie Masters, **165 Merrimac Trail, Apartment 6, Williamsburg, VA, 23185**.

53. On April 6, 2020, James City County Task Force Officer Richard Pennycuff conducted a physical surveillance at 7-11 on Bypass Road in Williamsburg VA and observed a blue Dodge Dart bearing Virginia Tags UYH-4825 parked out front. On April 7, 2020, a check through the Virginia DMV revealed the blue Dodge was registered to Timothy Cassidy, **165 Merrimac Trail, Apartment 6, Williamsburg, VA, 23185**.

54. On April 10, 2020, your affiant conducted a check through the Clear information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) for Timothy Cassidy. The check provided that Timothy

Cassidy resided at **165 Merrimac Trail, Apartment 6, Williamsburg, VA, 23185**. The check listed a previous residence held in Newport News, VA and a prior residence held at 165 Merrimac Trail, Apartment 3, Williamsburg, VA, 23185.

Conclusion

55. Based on the facts set forth above, your affiant believes probable cause exists that located at **165 Merrimac Trail, Apartment 6, Williamsburg, VA, 23185,** are violations of Title 18, United States Code, §§ 2252A(a)(2) and 2252A(a)(5)(B), provides any person who knowingly receives or distributes any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, shall be punished.

56. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities (more precisely described in Attachment B) of such violations will be found at the premises of **165 Merrimac Trail, Apartment 6, Williamsburg, VA, 23185** (more precisely described in Attachment A.)

57. Accordingly, your affiant requests that a search warrant be issued authorizing FBI agents, representatives of the FBI, with assistance from representatives of other law enforcement agencies as required, to search **165 Merrimac Trail, Apartment 6, Williamsburg, VA, 23185** (more precisely described in Attachment A), for evidence, fruits, and instrumentalities (more precisely described in Attachment B) of the offenses described in paragraphs 7-8 of this affidavit.

FURTHER AFFIANT SAYETH NOT.

Stacey A. Sullivan
Special Agent
FBI Child Exploitation Task Force

Federal Bureau of Investigation

This affidavit has been reviewed for legal sufficiency by Assistant United States Attorney Peter Osyf.

Reviewed: _____
Peter Osyf
Assistant United States Attorney

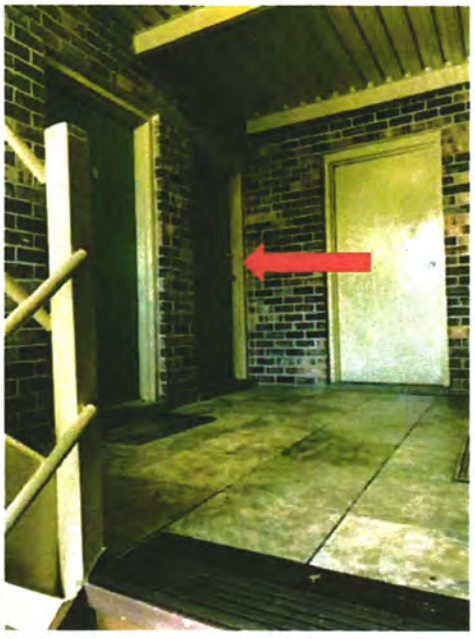
Subscribed and sworn before me this 16th day of April, 2020, in the City of Norfolk, Virginia.

_____
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is the property located at **165 Merrimac Trail, Apartment 6, Williamsburg, VA, 23185** (the "SUBJECT PREMISES") which is further described as an apartment located up the stairs of the Merrimac Trail apartment complex. The door is green with the number "6" located on a beige placard in the middle of the door. On the outside of the complex the numbers "165" are located to the left of the entrance way.



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, §§ 2252(a)(2) and 2252A(a)(5)(B):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including

a. Records, information, and items relating to the occupancy or ownership of, **165 Merrimac Trail, Apartment 6, Williamsburg, VA, 23185,** including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and

c. Records and information relating to sexual exploitation of children, including correspondence and communications between users of the web based picture gallery.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.